



DEPARTMENT OF THE AIR FORCE  
HEADQUARTERS AIR FORCE PERSONNEL CENTER  
RANDOLPH AIR FORCE BASE TEXAS

Dear Air Force Member

**It is very important that you read this entire letter as it contains information about recent unauthorized access to your personnel records.** As you may have heard by now, an unauthorized user accessed approximately 33,300 Assignment Management System (AMS) records in the May-June 2005 timeframe. **Your personal AMS record was one of the records accessed.** While not one incident of identity theft has been linked to this unauthorized access, we nevertheless want to make you aware of potential risks stemming from this incident and the steps we recommend you take to protect yourself against the risks.

I also want to assure you that immediately upon discovery of the unauthorized access, we removed the AMS from service so that a complete security review could be done. The AMS has now been returned to service, but with increased security measures. A criminal investigation also began immediately; we delayed sending you this notice for a short time in order to give our law enforcement officials the best opportunity in the early critical time period to catch the perpetrator(s).

Of immediate importance to you is the fact that your AMS record contains your Social Security number. While the AMS itself does not contain pay information, the data in AMS could potentially be used to gain access to other systems that control your military pay direct deposits and allotments. Based on these facts alone, I want to make you aware of the consumer protection steps which you may choose to use as discussed in this letter, including the Federal Trade Commission (FTC) attachment. In the interest of full disclosure, I also want you to know the accessed AMS records contained a number of items which are not subject to release without your consent under the Federal Privacy Act; such as marital status, number of dependents, date of birth, race/ethnic origin (if declared), civilian educational degrees and major areas of study, school and year of graduation, and duty information for overseas assignments or for routinely sensitive units.

What actions are available to you as a potential victim of identity theft?

- First, you may choose to file a "fraud alert" with the three major credit bureaus (Equifax, Experian and TransUnion) using the contact information in the attached FTC Fact Sheet. This will let creditors know to contact you before they open any new accounts in your name or make changes to your existing accounts. The fraud alert is automatically active for 90 days, and you may request an extension to this alert at any time.
- Second, you may request a *free* credit report from any of the three major credit bureaus using the contact information attached. Under the Fair Credit Reporting Act,


you are entitled to a free credit file disclosure by reason of this fraud alert incident. Credit reports are excellent tools to monitor unauthorized account activity.

- If at any point you believe your identity or account information has been misused, you should immediately report this to law enforcement personnel and to the Federal Trade Commission using the contact information in the FTC Fact Sheet. Further, you should contact the legal assistance function within the Staff Judge Advocate's office which services your unit to obtain an individualized plan to respond to your case. Legal assistance attorneys, equipped with current consumer protection information, can help you respond to specific instances of identity theft should it arise. This assistance is, of course, free to you as a resource to military personnel.

For the Air Force's part, we are conducting a wall-to-wall review of our personnel-related data systems to maximize security of the systems. This may cause some inconvenience to users as we increase our access requirements, but in the long run it will be our best way to protect our members against theft of personal information.

This is a challenge we will have to work together. Identity theft and other fraudulent uses of our resources steal from our operational budgets and endanger our mission. They also negatively impact our people. If you notice abnormalities or security issues on any of our systems, bring these to the attention of the systems administrator and your leadership immediately. While we very much regret any inconvenience or other problems this incident may cause, we are convinced that—working together—we will win the fight against identity theft and be a stronger Air Force from the experience.

You may contact the Air Force Personnel Contact Center toll free: 1(800) 616-3775 or commercial: (210) 565-5000 or DSN 665-5000 if you have general questions about this AMS incident.

  
ANTHONY F. PRZYBYLSKI  
Major General, USAF  
Commander

Attachment:  
FTC Identity Theft Information

## What To Do If Your Personal Information Has Been Compromised

Companies or institutions that keep personal information about you have an obligation to safeguard it. Still, from time to time, the personal information they hold may be accidentally disclosed or deliberately stolen. If your information falls into the wrong hands, it may be misused to commit fraud against you.

If you get a notice that your personal information may have been compromised, taking certain steps quickly can minimize the potential for the theft of your identity.

If the stolen information includes your Social Security number, call the toll-free fraud number of any one of the three nationwide consumer reporting companies and place an **initial fraud alert** on your credit reports. This alert can help stop someone from opening new credit accounts in your name.

**Equifax:** [www.equifax.com](http://www.equifax.com)

1-800-525-6285; P.O. Box 740241, Atlanta GA 30374-0241

**Experian:** [www.experian.com](http://www.experian.com)

1-888-EXPERIAN (397-3422); P.O. Box 2002, Allen TX 75013

**TransUnion:** [www.transunion.com](http://www.transunion.com)

1-800-680-7289; Fraud Victim Assistance Division  
P.O. Box 6790, Fullerton CA 92834-6790

An **initial fraud alert** stays on your credit report for 90 days. When you place this alert on your credit report with one nationwide consumer reporting company, you'll get information about ordering one free credit report from each of the companies. It's prudent to wait about a month after your information was stolen before you order your report. That's because suspicious activity may not show up right away. Once you get your reports, review them for suspicious activity, like inquiries from companies you didn't contact, accounts you didn't open, and debts on your accounts that you can't explain. Check that information—like your SSN, address(es), name or initials, and employers—is correct.

Once you've taken these precautions, watch for signs that your information is being misused. For example, you may not get certain bills or other mail on time. Follow up with creditors if your bills don't arrive on time. A missing bill could mean an identity thief has taken over your account and changed your billing address to cover his tracks.

Other signs include:

- receiving credit cards that you didn't apply for;
- being denied credit, or being offered less favorable credit terms, like a high interest rate, for no apparent reason; and
- getting calls or letters from debt collectors or businesses about merchandise or services you didn't buy.

Continue to read your financial account statements promptly and carefully, and to monitor your credit reports every few months in the first year of the theft, and once a year thereafter. For more information on getting your credit reports free once a year or buying additional reports, read *Your Access to Free Credit Reports* at <http://www.ftc.gov/bcp/online/pubs/credit/freereports.htm>.

If your information has been misused, file a report about your identity theft with the police, and file a complaint with the Federal Trade Commission at [www.consumer.gov/idtheft](http://www.consumer.gov/idtheft).

The FTC works for the consumer to prevent fraudulent, deceptive, and unfair business practices in the marketplace and to provide information to help consumers spot, stop, and avoid them. To file a complaint or to get free information on consumer issues, visit [www.ftc.gov](http://www.ftc.gov) or call toll-free 1-877-FTC-HELP (1-877-382-4357); TTY: 1-866-653-4261. The FTC enters Internet, telemarketing, identity theft, and other fraud-related complaints into Consumer Sentinel, a secure, online database available to hundreds of civil and criminal law enforcement agencies in the U.S. and abroad.

FOR THE CONSUMER 1-877-FTC-HELP

FEDERAL TRADE COMMISSION [www.ftc.gov](http://www.ftc.gov)

March 2005

**Obtaining free credit reports:**

To request a free annual disclosure, you may contact the Central Source on-line at <https://www.annualcreditreport.com>. You can also make the request by calling Central Source toll free at 1-877-FACTACT (322-8228), or by using the mail request form available at the Central Source website (<https://www.annualcreditreport.com>).